Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97

COMMENTS OF SECURUS TECHNOLOGIES, INC.

Securus Technologies, Inc. ("Securus"), by its undersigned counsel, submits these comments in response to the Declaratory Ruling and Third Further Notice of Proposed Rulemaking ("Declaratory Ruling and Third FNPRM") released in the above-captioned dockets on June 7, 2019, by the Federal Communications Commission ("FCC" or "Commission") and published in the Federal Register on June 24, 2019 (84 Fed. Reg. 29387). Securus commends the Commission's efforts to combat unlawful robocalls and urges the Commission to ensure that these efforts do not inadvertently harm consumers by blocking lawful and often important calls.

Securus provides phone, messaging, and video call technologies to more than 1.2 million inmates across North America, and serves over 3,400 public safety, law enforcement, and correction agencies. The Commission has consistently recognized that communications between inmates and their friends and families can have a meaningful impact on prisoner rehabilitation and recidivism. *See, e.g., Rates for Interstate Inmate Calling Services*, Report and Order and Further Notice of Proposed Rulemaking, 28 FCC Rcd 14107, 14130, para. 43. As Securus has previously explained, policies that interfere with the ability of inmates to successfully place outbound calls will have unintended harmful consequences, such as behavioral issues during incarceration that could jeopardize the safety and security of inmates and correctional officers alike.

Securus recognizes the importance of shielding consumers from unlawful and unwanted robocalls. But it is critical that, as the Commission continues its necessary work eliminating robocalls, it also safeguards the capability for inmates to successfully place calls to their friends, families, legal counsel, and other parties. As such, Securus urges the Commission to take a number of issues into consideration as it moves forward.

First, Securus urges the Commission to impose more specific requirements for "opt-out" capabilities in call-blocking programs. The Commission recently clarified that "voice service providers may offer opt-out call-blocking programs based on any reasonable analytics designed to identify unwanted calls" and required providers to "offer sufficient information so that consumers can make an informed choice as to whether they wish to remain in the program or opt out." Declaratory Ruling and Third FNPRM at paras. 33-34. Securus supports the Commission's suggested methods of providing informed choice as delineated in the Declaratory Ruling and Third FNPRM. However, absent *express* requirements for voice service providers beyond clear disclosure to consumers, Securus is concerned that consumers may not possess the requisite knowledge of opt-out call blocking for a truly "informed" choice. This is particularly the case where inmate calls may be inadvertently blocked, given that a recipient of such a call may be entirely unaware that calls from inmates have been blocked and inmates will face substantial hurdles in being able to rectify an erroneous block on their own.

Thus, the Commission should require that voice service providers: (1) post a disclosure on their website; (2) provide the Commission with the address of that website so that staff and interested third parties can evaluate the adequacy of the disclosure; and (3) require a mechanism be in place that ensures that consumers have actually received notice of this disclosure in addition to making the website available. As other commenters have noted, simply featuring the information on a website is "insufficient to ensure customers have notice and the information they

need to make an informed choice about participating in such programs." Petition for Clarification or Reconsideration of the Alarm Industry Communications Committee, *Advanced Methods to Target and Eliminated Unlawful Robocalls and Call Authentication Trust Anchor*, CG. Docket No. 17-59, WC Docket No. 17-97 (filed Jul. 8, 2019). Any call-blocking program should actively empower consumers with an accurate understanding of how they may be impacted.

Second, the Commission should further clarify the term "reasonable analytics" so that any "reasonable analytics" will not erroneously identify outbound inmate calls as unlawful robocalls. As Securus has previously explained, it is common for all inmate calls from a particular correctional facility to originate from a single telephone number. Additionally, when a recipient of an inmate call first answers the call, a response to an automated voice is required before the parties are able to speak to each other. Furthermore, many inmate calls may be placed within a short time frame. In short, many of the features identified by the Commission as reflecting unwanted calls are inherent in inmate communications. Declaratory Ruling and Third FNPRM at para. 35. Other parties have expressed similar concerns: for example, the American Bankers Association notes that a majority of automated outbound calls are placed in response to a customer's request, and occur in a large volume from one number over a short time. Letter from the American Bankers Association to Marlene H. Dortch, Secretary, *Advanced Methods to Target and Eliminated Unlawful Robocalls and Call Authentication Trust Anchor*, CG Docket No. 17-59, WC Docket No. 17-97 (filed Jun. 3, 2019) ("ABA Letter"). To remedy these potential complications, the Commission should ensure that any allowable analytic used by service providers is consistent among providers, and, furthermore, that the use of analytics does not adversely impact consumers, including recipients of inmate calls. Securus recommends the Commission facilitate this goal by standardizing and making public the thresholds used to determine whether a call should be blocked.

Although Securus supports implementation of the SHAKEN/STIR authentication framework as one of many tools that could be used to identify and block unlawful robocalls, the Commission should not permit voice service providers to block calls solely due to failed authentication pursuant to the SHAKEN/STIR Framework. Declaratory Ruling and Third FNPRM at paras. 49-62. Because authentication and verification through SHAKEN/STIR has not yet been widely deployed, and it is unclear when industry-wide deployment will be completed, there is insufficient evidence that blocking calls based solely on a lack of SHAKEN/STIR authentication would result in blocking of only illegitimate or illegal robocalls, and not the erroneous blocking of lawful and legitimate calls, including inmate calls. Before providing any additional safe harbor(s) for call blocking, the Commission must ensure that a mechanism is in place to detect and remedy the erroneous blocking of calls, as discussed further below. Indeed, during the Commission's recent summit on the SHAKEN/STIR Framework, panelists from industry (including representatives of voice service providers and companies that provide robocalls blocking analytics to industry) cautioned against use of SHAKEN/STIR authentication as the sole basis for blocking calls. For example, Scott Hambuchen, Chief Information Officer for First Orion, cautioned that SHAKEN/STIR requires further study and said that "just because a call comes through that has not had any authentication applied to it so it can't be verified, that doesn't make that a bad call." Similarly, Jonathan Nelson, Director Product Management for Hiya, stated that "one of the first challenges that always comes up is … there will be both good and bad calls" in each SHAKEN/STIR authentication tier. Mr. Hambuchen suggested "there is a lot of work to be done" as carriers implement SHAKEN/STIR, to determine how carriers and analytics systems should use the information gathered through use of the Framework. He said that First Orion is "not taking any action on just the fact alone that a call has been verified. You really don't want to do that just yet. And, so, it becomes another element in that entire analytic and decision process of

what am I going to do with this call?" The Commission should heed these warnings and refrain from allowing a safe harbor for call blocking based solely on failed caller ID authentication.

Although Securus intends to implement the SHAKEN/STIR Framework when the standards are sufficiently developed, Securus faces significant problems doing so at this time. As a non-interconnected VoIP provider, Securus does not have its own Operating Company Number ("OCN") nor the associated NPA-NXX numbering blocks. Rather, Securus relies on purchasing originating telephone numbers from other voice service providers. To Securus' knowledge, the SHAKEN/STIR Framework currently only permits the owner of an OCN to sign a call, although it anticipates the possibility that owners may delegate certificate/signing authority to qualified customers of OCN-owners. Securus has not been provided details from its underlying provider partners regarding if, or when, such delegation will be supported. Even more troubling is the fact that some providers of originating numbers have suggested they may refuse to sign some calls because Securus does not terminate calls on their networks (which would be impossible to do, because Securus provides originating calling only in accordance with the requirements imposed by correctional facilities). The Commission should be mindful of these concerns and the potential for flaws in implementation before it adopts policies and regulations underpinned by the SHAKEN/STIR Framework.

Third, Securus encourages the Commission to adopt specific requirements regarding opt-in "white lists." Declaratory Ruling and Third FNPRM at paras. 43-46. Securus applauds the Commission for proposing to incorporate protections for lawful and wanted calls in its Declaratory Ruling and Third FPNRM. But these protections may be insufficient. For example, it is unlikely that recipients of inmate calls would have the relevant, updated phone number(s) saved in their contact lists to begin with, particularly given that the recipients are never *placing* the calls to an inmate at a correctional facility. In addition, it is especially critical that persons who have just been

arrested are able to place calls to family, friends, and/or legal counsel; but those parties will not know the telephone number from which the inmate's call will originate.

Securus asserts that one method of mitigating these harms is for the Commission to adopt its proposal to create a "Critical Calls" list, which would prevent providers from blocking certain numbers altogether. Declaratory Ruling and Third FNPRM at paras. 63-69. Although inmate calls are distinguishable from calls from emergency service numbers, there are a finite number of correctional facilities across the country and a relatively small set of telephone numbers from which inmate calls originate such that these numbers could easily be included and updated on any Critical Calls list. A confidential list or database of Critical Calls telephone numbers that should not be blocked by voice service providers on a wholesale basis could be maintained by the Commission or an industry-led group. Securus acknowledges that although malicious actors may try to take advantage of Commission safeguards, including a confidential Critical Calls list, calls originating from correctional facilities are not susceptible to abuse because outbound inmate calling systems already include robust built-in call-blocking features and all calls originating from such facilities are actively monitored for security and other purposes. Moreover, the Commission could adopt a reasonable process that service providers must go through to have their telephone numbers included in the Critical Calls list to prevent bad actors from manipulating the system. For example, the Commission could require persons/entities seeking to be included on the Critical Calls list to provide documentation demonstrating that calls originating from the identified telephone numbers are legitimate calls. Moreover, keeping the Critical Calls list confidential and establishing strict protocols for access to the list could limit the ability for bad actors to spoof the telephone numbers included on the list.

Last, Securus is concerned that Commission procedures to address and remedy erroneous call-blocking may not protect consumers from overly aggressive call blocking practices, in

particular if the Commission provides a "safe harbor" for voice service providers who block calls based on the SHAKEN/STIR Framework. Ensuring a mechanism to remedy inappropriately blocked calls is especially important to protect inmates and recipients of their calls because these callers have no control over whether a call is authenticated under the SHAKEN/STIR Framework or why calls were blocked by call-blocking analytics programs. Securus supports recommendations from other commenters to require "sufficient notice of blocking to the caller and to the call recipient," as well as a "mechanism for prompt release of any erroneously blocked numbers." ABA Letter at 2. However, as compared to other callers, inmates are in a disadvantaged position regarding the ability to remedy an erroneous block because all calls they place are originated through the inmate calling system. Moreover, it will likely be impossible for inmates who want to challenge an erroneous block to contact the service provider that blocked the call due to the nature of inmate calling services (*i.e.*, the call begins with an automated message that must be responded to before the call is completed, inmates generally are only permitted to call numbers that have been pre-approved by the facility, etc.) especially if the inmate must call a general customer service number of another voice service provider to remedy the block. In the case of inmate calling services, the Commission should require prompt notice to the inmate calling service provider (*e.g.*, Securus) that identifies the telephone number of the call that was blocked and the time and date of the blocked call to enable the inmate calling service provider to investigate and promptly request a remedy for the blocked call. In addition to requiring voice service providers to provide prompt notice to the affected callers and recipients, Securus urges the Commission to implement a reasonable time frame (which should be measured in hours, not days) in which voice service providers must unblock lawful calls following receipt of a facially valid challenge, in order to mitigate unnecessary harm to consumers.

In conclusion, while Securus applauds the Commission and industry's efforts to stop the continued onslaught of illegal and unwanted robocalls, Securus remains concerned that legitimate calls will be swept up in call-blocking processes if the Commission does not carefully calibrate its rules and any safe harbors for providers that engage in call-blocking. Accordingly, the Commission must at a minimum enhance the consumer notification requirements for providers that seek to engage in call-blocking to ensure that consumers have actual knowledge of the consequences of call-blocking efforts. The Commission must also avoid providing a safe harbor for providers that use as-yet-undefined "reasonable analytics" or the SHAKEN/STIR Framework as a basis for blocking suspected robocalls. The Commission should also strongly consider requiring use of a Critical Calls list to ensure that voice service providers do not block telephone calls originating from certain trusted telephone numbers. Finally, the Commission must establish a robust and swift challenge process for consumers and other voice service providers to rectify erroneous blocking of legitimate calls.

Respectfully submitted,

/s/Andrew D. Lipman

Andrew D. Lipman
MORGAN, LEWIS & BOCKIUS LLP
1111 Pennsylvania Ave, NW
Washington, DC 20004
(202) 739-3000 (Tel)
(202) 739-3001 (Fax)
andrew.lipman@morganlewis.com

Counsel for Securus Technologies, Inc.

Dated: July 24, 2019